TO: Clerk's Office
UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

APPLICATION FOR LEAVE
TO FILE DOCUMENT UNDER SEAL

****

In re: Search of Electronic Devices in the Possession of the Federal Bureau of Investigation
-v.-

Docket Number

****

SUBMITTED BY: Plaintiff____ Defendant____ DOJ ✓
Name: Craig R. Heeren
Firm Name: U.S. Attorney's Office, Eastern District of New York
Address: 271 Cadman Plaza East
Brooklyn, NY 11201
Phone Number: 718-254-6467
E-Mail Address: craig.heeren@usdoj.gov

INDICATE UPON THE PUBLIC DOCKET SHEET: YES ___ NO ✓
If yes, state description of document to be entered on docket sheet:

A) If pursuant to a prior Court Order:
Docket Number of Case in Which Entered:
Judge/Magistrate Judge:
Date Entered:

B) If a new application, the statute, regulation, or other legal basis that authorizes filing under seal

Rule 41

ORDERED SEALED AND PLACED IN THE CLERK'S OFFICE, AND MAY NOT BE UNSEALED UNLESS ORDERED BY THE COURT.

DATED: Brooklyn , NEW YORK
June 7, 2020 Steven M. Gold

U.S. MAGISTRATE JUDGE

RECEIVED IN CLERK'S OFFICE
DATE

MANDATORY CERTIFICATION OF SERVICE:
A.) ___ A copy of this application either has been or will be promptly served upon all parties to this action, **B.)** ___ Service is excused by 31 U.S.C. 3730(b), or by the following other statute or regulation:_____; or **C.)** ✓ This is a criminal document submitted, and flight public safety, or security are significant concerns. (Check one)

6/7/2020
DATE

SIGNATURE

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of New York

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* ELECTRONIC DEVICES IN THE POSSESSION OF THE FEDERAL BUREAU OF INVESTIGATION, AS DESCRIBED IN ATTACHMENT A	)	Case No. 20 MJ 425

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of New York *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before June 20, 2020 *(not to exceed 14 days)*

❒ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Duty Magistrate Judge.
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____.

Date and time issued: 06/07/2020 12:34 pm

Steven M. Gold
Judge's signature

City and state: Brooklyn, New York

Hon. Steven M. Gold U.S.M.J.
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 20 MJ	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

Print Save As... Reset

ATTACHMENT A

The property to be searched is

a. One black LG smart cellular phone which contains the label "Cricket" on the back of the phone and which was seized from the person of DZENAN CAMOVIC pursuant to his arrest on or about June 3, 2020

b. One black Samsung mobile phone, IMEI # 358689100215795

c. One gold Samsung mobile phone, IMEI # 354255092268384

d. One Sandisk 64 GB hard drive

e. One Kingston 4 GB hard drive

f. One Samsung tablet, model SM-T520

g. One silver iPhone, Model A1660, FCC ID #BCG-E3085A, IMEI #359167078902529

h. One Polaroid tablet, model PMID1000B

i. Twenty-one (21) compact discs and digital video discs

of which items b. through i. were seized from a residence at 580 East 22nd Street, Brooklyn New York 11226, Apartment #5 pursuant to a consensual search on or about June 4, 2020 (hereinafter the "Subject Devices"). The Subject Devices are currently located in the possession of one or more agents from the Federal Bureau of Investigation in New York, New York.

This warrant authorizes the forensic examination of the Subject Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

All records on the Subject Devices, described in Attachment A, that were created, accessed, modified, sent or received from January 1, 2019 through the present, along with files that are not otherwise dated, that relate to violations of 18 U.S.C. § 231(a)(3) (obstruction of law enforcement officer related to civil disorder), 18 U.S.C. § 922(g)(5) (possession of a firearm by an illegal alien) and 18 U.S.C. § 2339B (provision of material support to a foreign terrorist organization) (collectively, the "Subject Offenses"), including motive evidence to commit the Subject Offenses, involving DZENAN CAMOVIC his co-conspirators, associates and others with or about whom they have communicated, including:

1. All records and information on the Subject Devices including names and telephone numbers, as well as the contents of all call logs, contact lists, text messages, messaging applications (including Facebook, Twitter, and mobile encrypted messaging applications such as WhatsApp), emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, Internet activity (including caches, browser history and cookies, firewall logs, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses), and other electronic media constituting evidence, fruits or instrumentalities of the Subject Offenses.

2. Evidence of user attribution showing who used or owned the Subject Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. Evidence regarding the user's state of mind, including whether and why he harbored any hostile views toward law enforcement and the NYPD.

4. Evidence of the user's close associates, including the individuals with whom he may have had contact in the days leading up to June 3, 2020.

5. Evidence of the user's location at the time he was using the Subject Devices.

6. Evidence indicating efforts to provide support to or promote the activities of terrorists and foreign terrorist organizations, including by committing acts of violence in support of such organizations.

7. Evidence regarding jihadist propaganda, including communications regarding support for extremist attacks and support for violent extremist groups, including al-Qaeda in the Arabian Peninsula and ISIS.

8. Evidence that may identify any additional coconspirators or aiders and abettors, including records that help reveal their whereabouts.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

RMT/AAS:CRH/JAM/JGH

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF ONE BLACK LG SMART CELLULAR PHONE WHICH CONTAINS THE LABEL "CRICKET" ON THE BACK OF THE PHONE AND WHICH WAS SEIZED FROM THE PERSON OF DZENAN CAMOVIC PURSUANT TO HIS ARREST ON OR ABOUT JUNE 3, 2020 (THE "LG DEVICE") ONE BLACK SAMSUNG MOBILE PHONE, IMEI # 358689100215795 ONE GOLD SAMSUNG MOBILE PHONE, IMEI # 354255092268384 ONE SANDISK 64 GB HARD DRIVE ONE KINGSTON 4 GB HARD DRIVE ONE SAMSUNG TABLET, MODEL SM-T520 ONE SILVER IPHONE, MODEL A1660, FCC ID #BCG-E3085A, IMEI #359167078902529 ONE POLAROID TABLET, MODEL PMID1000B TWENTY-ONE (21) COMPACT DISCS AND DIGITAL VIDEO DISCS IN THE POSSESSION OF THE FEDERAL BUREAU OF INVESTIGATION	APPLICATION FOR A SEARCH WARRANT FOR AN ELECTRONIC DEVICE Case No. 20 MJ 425

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Colin J. McLafferty, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of a supplemental application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing further examination of:

a. One black LG smart cellular phone which contains the label "Cricket" on the back of the phone and which was seized from the person of DZENAN CAMOVIC pursuant to his arrest on or about June 3, 2020 (the "LG Device")

b. One black Samsung mobile phone, IMEI # 358689100215795

c. One gold Samsung mobile phone, IMEI # 354255092268384

d. One Sandisk 64 GB hard drive

e. One Kingston 4 GB hard drive

f. One Samsung tablet, model SM-T520

g. One silver iPhone, Model A1660, FCC ID #BCG-E3085A, IMEI #359167078902529

h. One Polaroid tablet, model PMID1000B

i. Twenty-one (21) compact discs and digital video discs

of which items b. through i. were seized from a residence at 580 East 22nd Street, Brooklyn New York 11226, Apartment #5 pursuant to a consensual search on or about June 4, 2020 (collectively, the "Subject Devices"), as described in Attachment A, which are currently in law enforcement possession, and the extraction from the Subjects Devices of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") signed to the FBI's Joint Terrorism Task Force ("JTTF"). I have investigated crimes involving, among other things, terrorism and the illegal possession of firearms.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

4. The JTTF is investigating DZENAN CAMOVIC and others for an attack on multiple New York City Police Department ("NYPD") officers on or about June 3, 2020. The investigation involves violations of, among other statutes, 18 U.S.C. § 231(a)(3) (obstruction of law enforcement officer related to civil disorder), 18 U.S.C. § 922(g)(5) (possession of a firearm by an illegal alien) and 18 U.S.C. § 2339B (provision of material support to a foreign terrorist organization ("FTO")).

5. On or about June 3, 2020, at approximately 11:50 p.m., CAMOVIC approached two uniformed NYPD officers in the vicinity of 885 Flatbush Avenue in Brooklyn, New York. The two officers were assigned to an anti-looting post that evening, including the responsibility for enforcing the curfew. Security camera footage from the area shows CAMOVIC walking on Flatbush Avenue toward the intersection of Flatbush and Church Avenues. Upon reaching the corner of Flatbush and Church Avenues, CAMOVIC turned onto Church Avenue, where the two NYPD officers stood on patrol. The surveillance video shows that, upon turning the corner in the direction of the police officers, CAMOVIC immediately stabbed one of officers in the neck area with a knife he already had in his hand, and then began chasing the second officer, repeatedly and violently stabbing at the officer in a clear attempt to kill him.

CAMOVIC then ran back toward the first officer, whom he had already stabbed, and attempted to stab him again. A struggle ensued. Video footage from the officer's bodycam shows that CAMOVIC fought for control of the officer's service weapon and ultimately gained control of it and fired multiple shots at several officers, including at one or more officers who responded to the scene.

6. A review of bodycam footage revealed that at multiple points during his attack on the NYPD officers, CAMOVIC yelled "Allahu Akbar." Based on my knowledge, training and experience, I know that Allahu Akbar is an Arabic phrase that means "God is the greatest" and is frequently exclaimed by perpetrators of violent jihadist attacks during such attacks.

7. Law enforcement officers searched CAMOVIC's person incident to his arrest immediately after his attack on police on June 3, 2020, during which time they recovered the LG Device. On June 4, 2020, this Court issued a search warrant authorizing law enforcement agents to search the LG Device for evidence of the Subject Offenses.[1]

8. Additionally, pursuant to that investigation, several electronic devices and electronic media, including all of the Subject Devices apart from the LG Device, were recovered from CAMOVIC's residence at 580 East 22nd Street, Apartment #5 Brooklyn New, York 11226, pursuant to a consensual search. On June 5 and June 6, 2020, the Honorable Steven M. Gold, Magistrate Judge for the Eastern District of New York, granted two search warrants to search those items. See Exhibit 2 & 3 (the "June 5 and June 6 Warrants").

---

[1] A copy of the June 4 2020 search warrant (the "June 4 Warrant") and the affidavit in support of the warrant (the "June 4 Affidavit") are attached hereto as Exhibit 1 and hereby incorporated by reference.

9. Each of the warrants authorized a search for "[a]ll records on the Subject Devices [or LG Device], described in Attachment A, that relate to [the Subject Offenses], including motive evidence to commit the Subject Offenses, involving DZENAN CAMOVIC his co-conspirators, associates and others with or about whom they have communicated, committed between May 25, 2020 and the present" and identified specific categories of evidence to be seized. See Attachment B to Exhibits 1-3.

10. The purpose of this supplemental warrant is to seek authorization to review all files on the SUBJECT DEVICES that are were created, accessed, modified, sent or received from January 1, 2019 through the present, along with files that are not otherwise dated, for evidence of the Subject Offenses.

11. As explained more fully in the June 4 Affidavit, phone records and other evidence show that, inter alia CAMOVIC used the LG Device to exchange multiple text messages with several individuals in the hours before his attack on the police officers. See Exhibit 1.

12. Law enforcement agents are continuing to review the contents of the LG Device pursuant to the June 4, 2020 Warrant. An initial review of the LG Device has revealed that CAMOVIC downloaded and used an application called Orbot**.** Orbot is a mobile application used for the Tor network. Tor, in turn, is a computer network designed to facilitate anonymous communication over the Internet. The Tor network accomplishes this by routing a user's communications through a globally distributed network of relay computers, or proxies, rendering ineffective any conventional Internet Protocol ("IP") address-based methods of identifying users. To access the Tor network, a user installs specific Tor software. The Tor

network also enables users to operate hidden sites that operate similarly to conventional websites. The Tor network permits a user to conduct internet activity with a high degree of privacy and anonymity. As a result, the network is often used by individuals involved in criminal activity that want to obscure their identity and evade law enforcement.

13. Here, it appears that CAMOVIC downloaded and began using Orbot to connect to the Tor network on or about June 1, 2020—two days prior to his attack. CAMOVIC appears to have connected and used the application on several occasions thereafter. On or about June 2, 2020 at approximately 10:00 p.m. New York time – less than 24 hours before the attack – CAMOVIC deleted the application. It appears that CAMOVIC may have been attempting to delete evidence of his criminal activity.

14. Additionally, review of the LG Device also indicates that CAMOVIC downloaded and used a mobile application called Citizen shortly before the attack. Citizen is a social media application that allows users to send and receive information about local events associated with law enforcement activity. According to its website, Citizen describes itself as a "safety app that give you instant access to verified 911 information."

15. A user of the Citizen application located in or around the New York City region would receive alerts and information pertaining to NYPD law enforcement activity. In particular, during the relevant time period, a user of the Citizen application would have received information about NYPD activity related to the ongoing protests, looting and civil disorder. The application also allows users to submit and upload information and videos pertaining to such activity. The application provides mapping and location information for these events, and so a user would be able to learn about locations where NYPD are present.

16. CAMOVIC downloaded the Citizen application on June 2, 2020 and accessed the application on several occasions prior to his attack, including on June 3, 2020, shortly before the attack on law enforcement.

17. Additionally, according to records provided by the company that operates Citizen, CAMOVIC's service began on or about May 26, 2018, which indicates that CAMOVIC utilized Citizen on one or more previous mobile devices, such as the cellular phones found at his residence.

18. Based on the above, it appears that CAMOVIC was researching law enforcement-related activity shortly before he attacked the NYPD officers. Furthermore, based on my training and experience, I know that individuals associated with or supporting foreign terrorist organizations and involved in terrorist attacks will sometimes use technology like the Tor network to obtain information and communicate with one another.

19. Law enforcement agents are also continuing to review the contents of the Subject Devices found at CAMOVIC's residence pursuant to the June 5 and June 6 Warrants. A plain view review of these Subject Devices thus far has revealed that CAMOVIC was in possession of materials reflecting support for designated foreign terrorist organizations such as ISIS, and that CAMOVIC's interest in jihadist materials predates May 25, 2020.

20. For example, plain view review of the contents of the Sandisk 64 GB hard drive—which itself contained no label or date on the physical body of the items—revealed over 175 file folders and 15 images. According to data on the hard drive, each of these files reflected creation dates of March 29, 2019, and the majority of the files were last accessed on October 21, 2019.

21. Although investigating agents have not viewed or listened to the contents of these files, the file names on the Sandisk 64 GB hard drive appear related to extremist Salafi Islam religious content, including notable figures associated with designated foreign terrorist organizations. For example, the files include hundreds of audio files that, according to their file names, that based on my training, experience are files of speeches by Anwar al-Awlaki. For example, one file is titled "The Dust Will Never Settle Down." In a speech of that name, al-Awlaki advocated violence against individuals that he believed defamed and mocked Islam. Another filed, titled "Constants on the Path of Jihad" is the same title of another speech by al-Awlaki where he argued that the concept of "jihad" denoted combat against disbelievers rather than an internal struggle.

22. Also likely relevant to the mindset for CAMOVIC's attack is another file on the Sandisk 64 GB hard drive titled "Stop Police Terror."

23. Additionally, an audio files is titled, in Arabic text, "Salil al Sawarim," which I understand translates roughly into English as "The Clashing of Swords." I know that a song of that name was a popular Arabic song attributed to the ISIS.

24. Additionally, as discussed in the June 5 Warrant, see Exhibit 2, the 21 CDs included in the Subject Devices bear labels with descriptions such as "Abu Bakr 10" and "Young Aisha – Imam Anwar al A'wlaqi," reflecting that the contents of these files likely contains evidence of radical Islamic beliefs and evidence of support for foreign terrorist organizations like ISIS and AQAP.

JURISDICTION

25. The Subject Devices are currently located in the possession of one or more agents from the FBI in New York, New York. The Court has the authority to issue the attached warrants pursuant to Federal Rule of Criminal Procedure 41(b)(3), which states that a federal magistrate judge has authority to issue a search warrant "in an investigation of domestic terrorism or international terrorism – with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district."

26. The applied-for warrant would authorize the forensic examination of the Subject Devices for the purpose of identifying electronically stored data particularly described in Attachment B. The Subject Devices have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when they first came into the possession of the JTTF.

TECHNICAL TERMS

27. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to

and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage

media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication

devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be

assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

28. Based on my training, experience, and research, I know that the Subject Devices has capabilities that allow them to serve as wireless telephones, digital cameras, portable media players, GPS navigation devices, PDAs and tablets. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

29. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

30. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct

evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Subject Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Subject Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

b. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

c. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

d. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

31. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

32. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

33. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Subject Devices described in Attachment A to seek the items described in Attachment B.

REQUEST FOR SEALING

It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation that, even though the main target is already in custody, is still in an incipient phase, and it is possible that not all subjects of the investigation are aware of the nature of the government's investigation or the steps that it is taking to collect evidence. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

Colin McLafferty by SMG 06-07-2020

COLIN J. MCLAFFERTY
Special Agent, FBI

Subscribed and sworn to me by phone
on June 7, 2020:

Steven M. Gold

THE HONORABLE STEVEN M. GOLD
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is

a. One black LG smart cellular phone which contains the label "Cricket" on the back of the phone and which was seized from the person of DZENAN CAMOVIC pursuant to his arrest on or about June 3, 2020

b. One black Samsung mobile phone, IMEI # 358689100215795

c. One gold Samsung mobile phone, IMEI # 354255092268384

d. One Sandisk 64 GB hard drive

e. One Kingston 4 GB hard drive

f. One Samsung tablet, model SM-T520

g. One silver iPhone, Model A1660, FCC ID #BCG-E3085A, IMEI #359167078902529

h. One Polaroid tablet, model PMID1000B

i. Twenty-one (21) compact discs and digital video discs

of which items b. through i. were seized from a residence at 580 East 22nd Street, Brooklyn New York 11226, Apartment #5 pursuant to a consensual search on or about June 4, 2020 (hereinafter the "Subject Devices"). The Subject Devices are currently located in the possession of one or more agents from the Federal Bureau of Investigation in New York, New York.

This warrant authorizes the forensic examination of the Subject Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

All records on the Subject Devices, described in Attachment A, that were created, accessed, modified, sent or received from January 1, 2019 through the present, along with files that are not otherwise dated, that relate to violations of 18 U.S.C. § 231(a)(3) (obstruction of law enforcement officer related to civil disorder), 18 U.S.C. § 922(g)(5) (possession of a firearm by an illegal alien) and 18 U.S.C. § 2339B (provision of material support to a foreign terrorist organization) (collectively, the "Subject Offenses"), including motive evidence to commit the Subject Offenses, involving DZENAN CAMOVIC his co-conspirators, associates and others with or about whom they have communicated, including:

1. All records and information on the Subject Devices including names and telephone numbers, as well as the contents of all call logs, contact lists, text messages, messaging applications (including Facebook, Twitter, and mobile encrypted messaging applications such as WhatsApp), emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, Internet activity (including caches, browser history and cookies, firewall logs, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses), and other electronic media constituting evidence, fruits or instrumentalities of the Subject Offenses.

2. Evidence of user attribution showing who used or owned the Subject Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. Evidence regarding the user's state of mind, including whether and why he harbored any hostile views toward law enforcement and the NYPD.

4. Evidence of the user's close associates, including the individuals with whom he may have had contact in the days leading up to June 3, 2020.

5. Evidence of the user's location at the time he was using the Subject Devices.

6. Evidence indicating efforts to provide support to or promote the activities of terrorists and foreign terrorist organizations, including by committing acts of violence in support of such organizations.

7. Evidence regarding jihadist propaganda, including communications regarding support for extremist attacks and support for violent extremist groups, including al-Qaeda in the Arabian Peninsula and ISIS.

8. Evidence that may identify any additional coconspirators or aiders and abettors, including records that help reveal their whereabouts.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

RMT:DKK/JAM/JGH

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF A BLACK LG SMART CELLULAR PHONE, CURRENTLY IN THE POSSESSION OF THE JOINT TERRORISM TASK FORCE IN BROOKLYN, NEW YORK	APPLICATION FOR A SEARCH WARRANT FOR AN ELECTRONIC DEVICE Case No. 20 MJ 411

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Colin J. McLafferty, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and have been since July 2018. Since 2019, I have been assigned to the FBI's Joint Terrorism Task Force ("JTTF"). I have investigated crimes involving, among other things, terrorism and the illegal possession of firearms.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is a BLACK LG smart cellular phone which contains the label "Cricket" on the back of the phone and which was seized from the person of DZENAN CAMOVIC pursuant to his arrest on or about June 3, 2020, as described in greater detail herein (hereinafter the "Device"). The Device is currently located in the possession of one or more agents from the JTTF in Brooklyn, New York.

5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

BACKGROUND ON ISIS AND AQAP

6. On or about October 15, 2004, the United States Secretary of State designated al-Qaeda in Iraq ("AQI"), then known as Jam'at al Tawid wa' al-Jahid, as a Foreign Terrorist Organization ("FTO") under Section 219 of the Immigration and Nationality Act, and as a Specially Designated Global Terrorist entity under Section 1(b) of Executive Order 13224. On or about December 11, 2012, the Secretary of State amended the designation of AQI to include the following aliases: al-Nusrah Front ("ANF"), Jabhat al-Nusrah, Jabhet al-Nusra, The Victory Front, and Al-Nusrah Front for the People of the Levant.

7. On or about May 15, 2014, the Secretary of State, in response to the evolving nature of the relationships between ANF and AQI, amended the designation of AQI as an FTO under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist entity under section 1(b) of Executive Order 13224, to add the alias Islamic

State of Iraq and the Levant ("ISIL") as its primary name and to remove all aliases associated with al-Nusrah Front. The Secretary of State also added the following aliases to the FTO listing: The Islamic State of Iraq and al-Sham (ISIS - which is how the FTO will be referenced herein), The Islamic State of Iraq and Syria, ad-Dawla al-Islamiyya fi al-Iraq wa-sh-Sham, Daesh, Dawla al Islamiya, and Al-Furqan Establishment for Media Production. On September 21, 2015, the Secretary added the following aliases to the ISIS FTO listing: Islamic State, ISIL, and ISIS. To date, ISIS remains a designated FTO.

8. On January 19, 2010, the Secretary of State designated al-Qa'ida in the Arabian Peninsula (AQAP), also known as al-Qa'ida of Jihad Organization in the Arabian Peninsula, also known as Tanzim Qa'idat al-Jihad fi Jazirat al-Arab, also known as al-Qa'ida Organization in the Arabian Peninsula (AQAP), also known as al-Qa'ida in Yemen (AQY), also known as al-Qa'ida in the South Arabian Peninsula, as a Foreign Terrorist Organization ("FTO") under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist under section 1(b) of Executive Order 13224. To date, AQAP remains a designated FTO.

PROBABLE CAUSE

9. The JTTF is investigating DZENAN CAMOVIC and others for an attack on multiple New York City Police Department ("NYPD") officers on or about June 3, 2020. The investigation involves violations of, among other statutes, 18 U.S.C. § 231(a)(3) (obstruction of law enforcement officer related to civil disorder),[1] 18 U.S.C. § 922(g)(5) (possession of a

[1] Section 231(a)(3) provides, in relevant part: "(3)Whoever commits or attempts to commit any act to obstruct, impede, or interfere with any fireman or law enforcement officer lawfully engaged in the lawful performance of his official duties incident to and during the commission of a civil disorder which in any way or degree obstructs, delays, or adversely

firearm by an illegal alien) and 18 U.S.C. § 2339B (provision of material support to a foreign terrorist organization).

10. In or about late May 2020 and early June 2020, a series of demonstrations and protests occurred in New York City. These actions included the gathering of large crowds in Brooklyn, New York, including at night. Although the vast majority of individuals participating in these demonstrations have acted peacefully, a minority of individuals have engaged in looting, violence against law enforcement officers and other criminal conduct while the demonstrations were ongoing.

11. As a result of the demonstrations, hundreds of NYPD officers were deployed throughout New York City, including in Brooklyn. In addition, as a result of the civil unrest, on June 2, 2020, New York State Governor Andrew Cuomo and New York City Mayor Bill de Blasio announced a citywide curfew. NYPD officers helped to enforce the curfew. On June 3, 2020, a citywide curfew was in effect beginning at 8:00 p.m.

12. On or about June 3, 2020, at approximately 11:50 p.m., CAMOVIC approached two uniformed NYPD officers in the vicinity of 885 Flatbush Avenue in Brooklyn, New York. The two officers were assigned to an anti-looting post that evening, including the responsibility for enforcing the curfew. Security camera footage from the area shows CAMOVIC walking on Flatbush Avenue toward the intersection of Flatbush and Church Avenues. Upon reaching

---

affects commerce or the movement of any article or commodity in commerce or the conduct or performance of any federally protected function—Shall be fined under this title or imprisoned not more than five years, or both."

the corner of Flatbush and Church Avenues, CAMOVIC turned onto Church Avenue, where the two NYPD officers stood on patrol. The surveillance video shows that, upon turning the corner in the direction of the police officers, CAMOVIC immediately stabbed one of officers in the neck area with a knife he already had in his hand, and then began chasing the second officer, repeatedly and violently stabbing at the officer in a clear attempt to kill him. CAMOVIC then ran back toward the first officer, whom he had already stabbed, and attempted to stab him again. A struggle ensued. Video footage from the officer's bodycam shows that CAMOVIC fought for control of the officer's service weapon and ultimately gained control of it and fired multiple shots at several officers, including at one or more officers who responded to the scene.

13. CAMOVIC was ultimately shot by responding officers and taken in to custody.

14. A review of bodycam footage revealed that at multiple points during his attack on the NYPD officers, CAMOVIC yelled "Allahu Akbar." Based on my knowledge, training and experience, I know that Allahu Akbar is an Arabic phrase that means "God is the greatest" and is frequently exclaimed by perpetrators of violent jihadist attacks during such attacks.

15. On or about June 4, 2020, CAMOVIC's father provided consent to law enforcement officers to search his apartment, where CAMOVIC also resides. During a search of CAMOVIC's bedroom, which CAMOVIC's father has regular access to, officers discovered DVDs indicating that they contained violent jihadist propaganda. Specifically, officers observed multiple compact discs or DVDs marked "Abu Bakr," a possible reference to Abu Bakr al-Baghdadi, the now deceased self-proclaimed leader of the Islamic State in Iraq

and Syria ("ISIS"), a foreign terrorist organization that, since 2013, has claimed credit for numerous terrorist activities, including the November 2015 terrorist attacks in Paris, France, and the March 2016 suicide bombings in Brussels, Belgium, among many others. Officers also observed in CAMOVIC's room multiple compact discs or DVDs marked "Anwar al-Awlaki," including one that also included the word "jihad." Al-Awlaki was a United States-born radical Islamic cleric and prominent leader of the foreign terrorist organization al Qaeda in the Arabian Peninsula who was killed on or about September 30, 2011. Even now, nearly nine years after his death, al-Awlaki is still commonly regarded as the leading figure inciting English-speaking Muslims to participate in violent jihad.

16. Based on my knowledge, training and experience, the confident, aggressive and unprovoked nature of the attack, including his text message to Individual 1 immediately before the attack that he would "be a while" and the fact that he was already holding the knife which he immediately used to attack the officers, indicates that his attack on the officers was planned and premediated.

17. Law enforcement officers searched CAMOVIC's person incident to his arrest, during which time they recovered the Device.

18. Phone records and interviews of CAMOVIC's associates reflect that his cell phone number is 347-394-9934, which is the phone number for the Device.

19. The investigation has revealed that earlier on June 3, 2020, hours before his attack, CAMOVIC had dinner with two associates in Brooklyn (hereinafter "Individual 1" and "Individual 2") and that, after dinner, the three individuals separated. Toll records for the

Device as well as text messages and additional information provided to law enforcement by Individual 1 indicate that CAMOVIC exchanged messages with Individual 1 about possibly meeting again on the evening of June 3. At approximately 11:09 p.m., CAMOVIC texted Individual 1 asking about Individual 1's whereabouts. Individual 1 responded that he would be home soon and then wrote, "Wut up. Btw that shooting that u said, [Individual 2] called me B4 and said that cops came to him for cameras. Some guy killed to ppl."[2] CAMOVIC responded "damb" and then informed Individual 1 that he was on Ocean Avenue, near Individual 1's home. Individual 1 then responded "U waiting for me? Imma be there in like 5." CAMOVIC responded "kk" and then, at 11:38 p.m.—approximately 12 minutes before his attack on police—CAMOVIC wrote, "Ill be a while."

20. Based on a comparison of the toll records for the Device and the screenshots of text messages that Individual 1 provided to law enforcement, it appears that Individual 1 may have sent to the Device one additional text message at approximately 11:10 p.m. which was not captured in the screenshots Individual 1 provided to law enforcement. The toll records indicate that the apparently missing text message was sent by Individual 1 to CAMOVIC seconds before or seconds after Individual 1's text message to CAMOVIC that police had questioned Individual 2 about a shooting ("Btw that shooting that u said, [Individual 2] called me B4 and said that cops came to him for cameras. Some guy killed to ppl.").

---

[2] Law enforcement officers are attempting to identify the shooting incident that Individual 1 referred to in his June 3, 2020 text message to CAMOVIC.

21. Toll records for the Device further show that, in addition to his communications with Individual 1 immediately before the attack, CAMOVIC also used the Device to exchange multiple text messages with another other individual ("Individual 3") in the hours before the attack. Specifically, toll records for the Device show that CAMOVIC used the device to exchange approximately five text messages with Individual 3 between approximately 7:00 and 10:00 p.m. on June 3, 2020.

22. Immigration records associated with CAMOVIC's father show that CAMOVIC was born outside of the United States and has no legal immigration status in the United States. Accordingly, CAMOVIC likely violated 18 U.S.C. § 922(g)(5), which prohibits illegal aliens from possessing firearms, in attempting to take control of and firing an NYPD officer's service weapon.

23. Based on my training and experience, I know that individuals who plan attacks on law enforcement often use cellular phones to do so, including by communicating with others regarding their attack plans, researching and locating targets, planning their route of attack and/or escape, searching for weapons and posting content on social media regarding their mental state and intentions. There is also probable cause to believe that, because CAMOVIC was carrying the Device on his person at the time of the attack, the Device will contain evidence of his location immediately prior to the attack and possibly whether and where he met with any coconspirators before the attack. Furthermore, there is probable cause to believe that the text messages stored on the Device will resolve the apparent discrepancy between the toll records for the Device and the screenshots of text messages provided to law enforcement

by Individual 1. As noted above, these texts appear to relate to a shooting and to statements made to law enforcement officers investigating said shooting.

24. Based on the foregoing, I submit that this affidavit establishes probable cause to search the Device. Your affiant is further requesting to share the information obtained from this search warrant (to include copies of digital media and social media applications) with any government agency investigating, or aiding in the investigation, or this case or related matters.

25. The Device is currently in the possession of the JTTF in Brooklyn, New York. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the JTTF.

TECHNICAL TERMS

26. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless

telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage

media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing

computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a

telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

h. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

i. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

27. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

28. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

29. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

b. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

c. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

d. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

30. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

31. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

32. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

REQUEST FOR SEALING

It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation as not all of the subjects and targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

Colin J. McLafferty

COLIN J. MCLAFFERTY
Special Agent, FBI

Subscribed and sworn to me by phone
on June 4, 2020:

Steven M. Gold

THE HONORABLE STEVEN M. GOLD
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is a BLACK LG smart cellular phone which contains the label "Cricket" on the back of the phone and which was seized from the person of DZENAN CAMOVIC pursuant to his arrest on or about June 3, 2020, as described in greater detail herein (hereinafter the "Device"). The Device is currently located in the possession of the Joint Terrorism Task Force in Brooklyn New York.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

All records on the Device, described in Attachment A, that relate to violations of 18 U.S.C. § 231(a)(3) (obstruction of law enforcement officer related to civil disorder), 18 U.S.C. § 922(g)(5) (possession of a firearm by an illegal alien) and 18 U.S.C. § 2339B (provision of material support to a foreign terrorist organization) (collectively, the "Subject Offenses"), including motive evidence to commit the Subject Offenses, involving DZENAN CAMOVIC his co-conspirators, associates and others with or about whom they have communicated, committed between May 25, 2020 and the present, including:

1. All records and information on the Device including names and telephone numbers, as well as the contents of all call logs, contact lists, text messages, messaging applications (including Facebook, Twitter, and mobile encrypted messaging applications such as WhatsApp), emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, Internet activity (including caches, browser history and cookies, firewall logs, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses), and other electronic media constituting evidence, fruits or instrumentalities of the Subject Offenses.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. Evidence regarding the user's state of mind, including whether and why he harbored any hostile views toward law enforcement and the NYPD.

4. Evidence of the user's close associates, including the individuals with whom he may have had contact in the days leading up to June 3, 2020.

5. Evidence indicating efforts to provide support to or promote the activities of terrorists and foreign terrorist organizations, including by committing acts of violence in support of such organizations.

6. Evidence regarding jihadist propaganda, including communications regarding support for extremist attacks and support for violent extremist groups, including al-Qaeda in the Arabian Peninsula and ISIS.

7. Location information for the Device from 12:00 p.m. on June 3, 2020 to 12:00 a.m. on June 4, 2020.

8. Evidence that may identify any additional coconspirators or aiders and abettors, including records that help reveal their whereabouts.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

RMT/AAS:CRH/JAM/JGH

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF ONE BLACK SAMSUNG MOBILE PHONE, IMEI # 358689100215795; ONE GOLD SAMSUNG MOBILE PHONE, IMEI # 354255092268384; ONE SANDISK 64 GB HARD DRIVE; ONE KINGSTON 4 GB HARD DRIVE; ONE SAMSUNG TABLET, MODEL SM-T520; ONE SILVER IPHONE, MODEL A1660, FCC ID #BCG-E308512; ONE POLAROID TABLE, MODEL PMID1000B; AND TWENTY-ONE (21) COMPACT DISCS AND DIGITAL VIDEO DISCS IN THE POSSESSION OF THE JOINT TERRORISM TASK FORCE IN BROOKLYN, NEW YORK	APPLICATION FOR A SEARCH WARRANT FOR AN ELECTRONIC DEVICE Case No. 20 MJ 414

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Colin J. McLafferty, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—several electronic devices, as more fully set forth in Attachment A—which are currently in law

enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and have been since July 2018. Since 2019, I have been assigned to the FBI's Joint Terrorism Task Force ("JTTF"). I have investigated crimes involving, among other things, terrorism and the illegal possession of firearms.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The property to be searched is

a. One black Samsung mobile phone, IMEI # 358689100215795

b. One gold Samsung mobile phone, IMEI # 354255092268384

c. One Sandisk 64 GB hard drive

d. One Kingston 4 GB hard drive

e. One Samsung tablet, model SM-T520

f. One silver iPhone, Model A1660, FCC ID #BCG-E308512

g. One Polaroid tablet, model PMID1000B

h. Twenty-one (21) compact discs and digital video discs

recovered from 580 East 22nd Street, Brooklyn New York 11226, Apartment #5 (hereinafter the "Subject Devices") pursuant to a consensual search. The Subject Devices are currently located in the possession of one or more agents from the JTTF in Brooklyn, New York.

5. The applied-for warrant would authorize the forensic examination of the Subject Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

BACKGROUND ON ISIS AND AQAP

6. On or about October 15, 2004, the United States Secretary of State designated al-Qaeda in Iraq ("AQI"), then known as Jam'at al Tawid wa' al-Jihad, as a Foreign Terrorist Organization ("FTO") under Section 219 of the Immigration and Nationality Act, and as a Specially Designated Global Terrorist entity under Section 1(b) of Executive Order 13224. On or about December 11, 2012, the Secretary of State amended the designation of AQI to include the following aliases: al-Nusrah Front ("ANF"), Jabhat al-Nusrah, Jabhet al-Nusra, The Victory Front, and Al-Nusrah Front for the People of the Levant.

7. On or about May 15, 2014, the Secretary of State, in response to the evolving nature of the relationships between ANF and AQI, amended the designation of AQI as an FTO under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist entity under section 1(b) of Executive Order 13224, to add the alias Islamic State of Iraq and the Levant ("ISIL") as its primary name and to remove all aliases associated with al-Nusrah Front. The Secretary of State also added the following aliases to the FTO listing: The Islamic State of Iraq and al-Sham (ISIS - which is how the FTO will be referenced herein), The Islamic State of Iraq and Syria, ad-Dawla al-Islamiyya fi al-Iraq wa-sh-Sham, Daesh, Dawla al Islamiya, and Al-Furqan Establishment for Media Production. On September 21, 2015, the Secretary added the following aliases to the ISIS FTO listing: Islamic State, ISIL, and ISIS. To date, ISIS remains a designated FTO.

8. On January 19, 2010, the Secretary of State designated al-Qaeda in the Arabian Peninsula (AQAP), also known as al-Qaeda of Jihad Organization in the Arabian Peninsula, also known as Tanzim Qa'idat al-Jihad fi Jazirat al-Arab, also known as al-Qaeda Organization in the Arabian Peninsula (AQAP), also known as al-Qaeda in Yemen (AQY), also known as al-Qaeda in the South Arabian Peninsula, as a Foreign Terrorist Organization ("FTO") under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist under section 1(b) of Executive Order 13224. To date, AQAP remains a designated FTO.

PROBABLE CAUSE

9. The JTTF is investigating DZENAN CAMOVIC and others for an attack on multiple New York City Police Department ("NYPD") officers on or about June 3, 2020. The investigation involves violations of, among other statutes, 18 U.S.C. § 231(a)(3) (obstruction of law enforcement officer related to civil disorder),[1] 18 U.S.C. § 922(g)(5) (possession of a firearm by an illegal alien) and 18 U.S.C. § 2339B (provision of material support to a foreign terrorist organization).

10. In or about late May 2020 and early June 2020, a series of demonstrations and protests occurred in New York City. These actions included the gathering of large crowds in

[1] Section 231(a)(3) provides, in relevant part: "(3)Whoever commits or attempts to commit any act to obstruct, impede, or interfere with any fireman or law enforcement officer lawfully engaged in the lawful performance of his official duties incident to and during the commission of a civil disorder which in any way or degree obstructs, delays, or adversely affects commerce or the movement of any article or commodity in commerce or the conduct or performance of any federally protected function—Shall be fined under this title or imprisoned not more than five years, or both."

Brooklyn, New York, including at night. Although the vast majority of individuals participating in these demonstrations have acted peacefully, a minority of individuals have engaged in looting, violence against law enforcement officers and other criminal conduct while the demonstrations were ongoing.

11. As a result of the demonstrations, hundreds of NYPD officers were deployed throughout New York City, including in Brooklyn. In addition, as a result of the civil unrest, on June 1, 2020, New York State Governor Andrew Cuomo and New York City Mayor Bill de Blasio announced a citywide curfew. NYPD officers helped to enforce the curfew. On June 2, 2020, a citywide curfew was in effect beginning at 8:00 p.m.

12. On or about June 3, 2020, at approximately 11:50 p.m., CAMOVIC approached two uniformed NYPD officers in the vicinity of 885 Flatbush Avenue in Brooklyn, New York. The two officers were assigned to an anti-looting post that evening, including the responsibility for enforcing the curfew. Security camera footage from the area shows CAMOVIC walking on Flatbush Avenue toward the intersection of Flatbush and Church Avenues. Upon reaching the corner of Flatbush and Church Avenues, CAMOVIC turned onto Church Avenue, where the two NYPD officers stood on patrol. The surveillance video shows that, upon turning the corner in the direction of the police officers, CAMOVIC immediately stabbed one of officers in the neck area with a knife he already had in his hand, and then began chasing the second officer, repeatedly and violently stabbing at the officer in a clear attempt to kill him. CAMOVIC then ran back toward the first officer, whom he had already stabbed, and attempted to stab him again. A struggle ensued. Video footage from the officer's bodycam shows that CAMOVIC fought for control of the officer's service weapon and ultimately gained control of

it and fired multiple shots at several officers, including at one or more officers who responded to the scene.

13. CAMOVIC was ultimately shot by responding officers and taken in to custody.

14. A review of bodycam footage revealed that, at multiple points during his attack on the NYPD officers, CAMOVIC yelled "Allahu Akbar." Based on my knowledge, training and experience, I know that Allahu Akbar is an Arabic phrase that means "God is the greatest" and is frequently exclaimed by perpetrators of violent jihadist attacks during such attacks.

15. Based on my knowledge, training and experience, the confident, aggressive and unprovoked nature of the attack, including his text message to a third party immediately before the attack that he would "be a while," see infra paragraph 18, and the fact that he was already holding the knife which he immediately used to attack the officers, indicates that his attack on the officers was planned and premediated.

16. Law enforcement officers searched CAMOVIC's person incident to his arrest, during which time they recovered a black LG smart cellular phone (the "LG Phone").

17. Phone records and interviews of CAMOVIC's associates reflect that the LG Phone was used to communicate with other individuals immediately prior to the attack.

18. Specifically, earlier on June 3, 2020, hours before his attack, CAMOVIC had dinner with two associates in Brooklyn (hereinafter "Individual 1" and "Individual 2") and that, after dinner, the three individuals separated. Toll records for the LG Phone as well as text messages and additional information provided to law enforcement by Individual 1 indicate that CAMOVIC exchanged messages with Individual 1 about possibly meeting again on the evening of June 3. At approximately 11:09 p.m., CAMOVIC texted Individual 1 asking about

Individual 1's whereabouts. Individual 1 responded that he would be home soon and then wrote, "Wut up. Btw that shooting that u said, [Individual 2] called me B4 and said that cops came to him for cameras. Some guy killed to ppl."[2] CAMOVIC responded "damb" and then informed Individual 1 that he was on Ocean Avenue, near Individual 1's home. Individual 1 then responded "U waiting for me? Imma be there in like 5." CAMOVIC responded "kk." and then, at 11:38 p.m.—approximately 12 minutes before his attack on police—CAMOVIC wrote, "Ill be a while."

19. Toll records for the phone number associated with the LG Phone further show that, in addition to his communications with Individual 1 immediately before the attack, CAMOVIC also used the LG Phone to exchange multiple text messages with another other individual ("Individual 3") in the hours before the attack. Specifically, toll records for the phone number associated with the LG Phone show that CAMOVIC used the device to exchange approximately five text messages with Individual 3 between approximately 7:00 and 10:00 p.m. on June 3, 2020.

20. On June 4, 2020, Magistrate Judge Steven M. Gold of the Eastern District of New York authorized a search warrant as to the LG Phone. See 20-MJ-411 (under seal).

21. Immigration records associated with CAMOVIC's father show that CAMOVIC was born outside of the United States and has no legal immigration status in the United States. Accordingly, CAMOVIC likely violated 18 U.S.C. § 922(g)(5), which prohibits illegal aliens

---

[2] Law enforcement officers are attempting to identify the shooting incident that Individual 1 referred to in his June 3, 2020 text message to CAMOVIC.

from possessing firearms, in attempting to take control of and firing an NYPD officer's service weapon.

22. On or about June 4, 2020, CAMOVIC's father provided written consent to law enforcement officers to search his apartment, located at 580 E. 22nd Street, Brooklyn, New York 11226, Apartment #5, where CAMOVIC also resides.

23. The consensual search encompassed, among other locations in the residence, a room that CAMOVIC's father identified as CAMOVIC's bedroom. CAMOVIC's father stated that he also had regular access to CAMOVIC's bedroom.

24. A search of CAMOVIC's bedroom revealed two knives. A third knife, which had a handle that resembled the knife used in the attack and therefore appeared to be from the same knife set, was observed and seized from an area near the kitchen of the residence.

The Subject Devices

25. Law enforcement officers discovered 21 compact discs ("CDs") or digital video discs ("DVDs") in CAMOVIC's bedroom with labels reflecting violent jihadist propaganda or content. Specifically, officers observed multiple CDs or DVDs marked "Abu Bakr," a possible reference to Abu Bakr al-Baghdadi, the now deceased self-proclaimed leader of ISIS. Officers also observed in CAMOVIC's bedroom multiple CDs or DVDs marked "Anwar al-Awlaki," including one that also included the word "jihad." Al-Awlaki was a United States-born radical Islamic cleric and prominent leader of the foreign terrorist organization al-Qaeda in the Arabian Peninsula who was killed on or about September 30, 2011. Even now, nearly nine years after his death, al-Awlaki is still commonly regarded as the leading figure inciting English-speaking Muslims to participate in violent jihad.

26. These 21 CDs or DVDs were located together in the same box and labeled as follows:

a. "Clearing the Fog: How to Respond to the Misconceptions About Islam" by "Yusha Evans." Information publically available on the internet identifies Yusha Evans as a radical Islamist preacher;

b. "Weakness of Faith and Its Cures" by Yusha Evans;

c. "Young Aisha – Imam Anwar al A'wlaqi" [al-Awlaki];

d. "Abu Bakr 4" written in marker;

e. "Abu Bakr 10" written in marker;

f. Bosnian-language title, including "Hafiz Muhammed Porca." Information publically available on the internet identifies Hafiz Muhammed Proca as a radical Islamist preacher;

g. "Galaxia International Services Inc. Money Transmitter," accompanied by Arabic language script and an address in Queens;

h. "Lives of the Prophets, Part 1, Anwar al- Awlaki";

i. "Lives of the Prophets, Volumes 3 and 4, Anwar al- Awlaki";

j. Bosnian-language words written in marker;

k. "The Life of Muhammad" on a printed on a sticker;

l. "Abu Bakr 5" written in marker;

m. "Abu Bakr 14" written in marker;

n. "Abu Bakr 9" written in marker;

o. "Al-Iman" with Arabic script;

p. A second disc reading "Al-Iman" with Arabic script;

q. Bosnian-language print, including the words "il tewhid," which is an armed Islamist insurgent group fighting in Syria;

r. Arabic-language script with a graphic of the Ka'aba in Mecca;

s. Bosnian-language print overlaid against a blue sky and grass background;

t. "The Life of Abu Bakr" printed on a sticker;

u. "Jihad Shaykh Anwar al Awlaki MP3 Borba" written in marker;

27. Officers also discovered several electronic devices in CAMOVIC's room, including the following:

a. One black Samsung mobile phone, IMEI # 358689100215795

b. One gold Samsung mobile phone, IMEI # 354255092268384

c. One Sandisk 64 GB hard drive

d. One Kingston 4 GB hard drive

e. One Samsung tablet, model SM-T520

f. One silver iPhone, Model A1660, FCC ID #BCG-E308512

g. One Polaroid tablet, model PMID1000B

28. Based on my training and experience, I know that individuals who provide support to foreign terrorist organizations, as well as individuals who plan and conduct terrorist attacks, often use multiple cellular phones and other electronic devices. They do so as a form of operational security, to compartmentalize evidence of their criminal activity and prevent the full details of their conduct from being revealed if one device is discovered by law enforcement.

29. Additionally, based on my training and experience, I know that mobile devices and tablets, like those recovered from CAMOVIC's bedroom, are often used by individuals associated with foreign terrorist organization and individuals involved in planning and conducting terrorist attacks for multiple purposes, including for communicating with others regarding their attack plans, researching and locating targets, planning their route of attack and/or escape, searching for weapons and posting content on social media regarding their mental state and intentions.

30. Additionally, based on my training and experience, I know that hard drives, such as the two hard drives recovered from CAMOVIC's bedroom, are often used by supporters of foreign terrorist organizations to store materials associated with violent jihadist propaganda. Additionally, individuals involved in planning and conducting terrorist attacks often use such hard drives to store materials useful for conducting attacks, such as instructions for building weapons or devices to use in an attack.

31. Finally, based on my training and experience, I know that individuals involved in terrorist attacks often draft and leave behind documents describing why they intended to commit such an attack, in the belief that they will die in the course of such an attack.

32. Based on the foregoing, I submit that this affidavit establishes probable cause to search the Subject Devices. Your affiant is further requesting to share the information obtained from this search warrant (to include copies of digital media and social media applications) with any government agency investigating, or aiding in the investigation, or this case or related matters.

33. The Subject Devices are currently in the possession of one or more JTTF agents in Brooklyn, New York. In my training and experience, I know that the Subject Devices have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Subject Devices first came into the possession of the JTTF.

TECHNICAL TERMS

34. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones

may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been.

Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing

documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet,

connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

35. Based on my training, experience, and research, I know that several of the Subject Devices have capabilities that allow them to to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, PDA and tablet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

36. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

37. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Subject Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Subject Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

b. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

c. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

d. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

38. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose

many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

39. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

40. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Subject Devices described in Attachment A to seek the items described in Attachment B.

REQUEST FOR SEALING

It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation that, even though the main target is already in custody, is still in an incipient phase, and it is possible that not all subjects of the investigation are aware of the nature of the government's investigation or the steps that it is taking to collect evidence. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate. Premature disclosure of the contents of this

affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

COLIN J. MCLAFFERTY
Special Agent, FBI

Subscribed and sworn to me by phone
on June 5, 2020:

Steven M. Gold

THE HONORABLE STEVEN M. GOLD
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is

1. One black Samsung mobile phone, IMEI # 358689100215795
2. One gold Samsung mobile phone, IMEI # 354255092268384
3. One Sandisk 64 GB hard drive
4. One Kingston 4 GB hard drive
5. One Samsung tablet, model SM-T520
6. One silver iPhone, Model A1660, FCC ID #BCG-E308512
7. One Polaroid tablet, model PMID1000B
8. Twenty-four (21) compact discs or digital video discs

which were seized from a residence at 580 East 22nd Street, Brooklyn New York 11226, Apartment #5 pursuant to a consensual search on or about June 4, 2020 (hereinafter the "Subject Devices"). The Subject Devices are currently located in the possession of one or more agents from the Joint Terrorism Task Force in Brooklyn, New York.

This warrant authorizes the forensic examination of the Subject Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

All records on the Subject Devices, described in Attachment A, that relate to violations of 18 U.S.C. § 231(a)(3) (obstruction of law enforcement officer related to civil disorder), 18 U.S.C. § 922(g)(5) (possession of a firearm by an illegal alien) and 18 U.S.C. § 2339B (provision of material support to a foreign terrorist organization) (collectively, the "Subject Offenses"), including motive evidence to commit the Subject Offenses, involving DZENAN CAMOVIC his co-conspirators, associates and others with or about whom they have communicated, committed between May 25, 2020 and the present, including:

1. All records and information on the Subject Devices including names and telephone numbers, as well as the contents of all call logs, contact lists, text messages, messaging applications (including Facebook, Twitter, and mobile encrypted messaging applications such as WhatsApp), emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, Internet activity (including caches, browser history and cookies, firewall logs, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses), and other electronic media constituting evidence, fruits or instrumentalities of the Subject Offenses.

2. Evidence of user attribution showing who used or owned the Subject Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. Evidence regarding the user's state of mind, including whether and why he harbored any hostile views toward law enforcement and the NYPD.

4. Evidence of the user's close associates, including the individuals with whom he may have had contact in the days leading up to June 3, 2020.

5. Evidence indicating efforts to provide support to or promote the activities of terrorists and foreign terrorist organizations, including by committing acts of violence in support of such organizations.

6. Evidence regarding jihadist propaganda, including communications regarding support for extremist attacks and support for violent extremist groups, including al-Qaeda in the Arabian Peninsula and ISIS.

7. Evidence that may identify any additional coconspirators or aiders and abettors, including records that help reveal their whereabouts.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

RMT/AAS:CRH/JAM/JGH

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF A PHILLIPS VOICETRACER DIGITAL RECORDER, SERIAL NUMBER DVT11100282135, AND A SILVER IPHONE, MODEL A1660, FCC ID #BCG-E3085A, IMEI #359167078902529 IN THE POSSESSION OF THE JOINT TERRORISM TASK FORCE	APPLICATION FOR A SEARCH WARRANT FOR AN ELECTRONIC DEVICE Case No. 20 MJ

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Colin J. McLafferty, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of a Phillips Voicetracer Digital Recorder, DVT11100282135 (the "Target Recording Device"), and a silver iPhone, Model A1660, FCC ID #BCG-E3085A, IMEI #359167078902529 (the "Target iPhone") (collectively, the "Target Devices"), as described in Attachment A, which are currently in law enforcement possession, and the extraction from the Target Devices of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") signed to the FBI's Joint Terrorism Task Force ("JTTF"). I have investigated crimes involving, among other things, terrorism and the illegal possession of firearms.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

4. The JTTF is investigating DZENAN CAMOVIC and others for an attack on multiple New York City Police Department ("NYPD") officers on or about June 3, 2020. The investigation involves violations of, among other statutes, 18 U.S.C. § 231(a)(3) (obstruction of law enforcement officer related to civil disorder), 18 U.S.C. § 922(g)(5) (possession of a firearm by an illegal alien) and 18 U.S.C. § 2339B (provision of material support to a foreign terrorist organization ("FTO")).

5. Pursuant to that investigation, numerous electronic devices and electronic media, including the Target Devices, were recovered from 580 East 22nd Street, Brooklyn New York 11226, Apartment #5 pursuant to a consensual search. On June 26, 2020, the Honorable Steven M. Gold, Magistrate Judge for the Eastern District of New York, granted warrants to search those items (20-MJ-414) (under seal). The application and warrants, attached and incorporated into the instant application by reference herein, inadvertently omitted the Target Recording Device. Additionally, the serial number of the Target iPhone had two incorrect characters, reading "BCG-E308512" instead of "BCG-E3085A."

6. Based on my training and experience, I know that individuals from the United States and Western countries who wish to support FTOs, including the Islamic State of Iraq and al-Sham ("ISIS"), will often make a recording pledging allegiance to the FTO. Additionally, I know based on my training and experience that, prior to engaging in a terrorist attack, the attacker will often record a message explaining that the attack is inspired by or being

conducted on behalf of the FTO, or describing why they intended to commit such an attack, in the belief that they will die in the course of such an attack.

JURISDICTION

7. The Target Devices are currently located in the possession of one or more agents from the FBI in New York, New York. The Court has the authority to issue the attached warrants pursuant to Federal Rule of Criminal Procedure 41(b)(3), which states that a federal magistrate judge has authority to issue a search warrant "in an investigation of domestic terrorism or international terrorism – with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district."

8. The applied-for warrant would authorize the forensic examination of the Target Devices for the purpose of identifying electronically stored data particularly described in Attachment B. The Target Devices have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when they first came into the possession of the JTTF.

TECHNICAL TERMS

9. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones

or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio,

video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

10. Based on my training, experience, and research, I know that the Target iPhone has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, PDA and tablet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

11. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed

via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

12. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Target Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Target Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

b. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

c. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a

computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

d. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

13. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

14. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

15. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Target Devices described in Attachment A to seek the items described in Attachment B.

REQUEST FOR SEALING

It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation that, even though the main target is already in custody, is still in an incipient phase, and it is possible that not all subjects of the investigation are aware of the nature of the government's investigation or the steps that it is taking to collect evidence. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

COLIN J. MCLAFFERTY
Special Agent, FBI

Subscribed and sworn to me by phone
on June 6, 2020:

Steven M. Gold

THE HONORABLE STEVEN M. GOLD
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is

1. a Phillips Voicetracer Digital Recorder, Serial Number DVT11100282135 (the "Target Recording Device"); and
2. a silver iPhone, Model A1660, FCC ID #BCG-E3085A, IMEI #359167078902529 (the "Target iPhone")

which were seized from a residence at 580 East 22nd Street, Brooklyn New York 11226, Apartment #5 pursuant to a consensual search on or about June 4, 2020 (hereinafter the "Target Devices"). The Target Devices are currently located in the possession of one or more agents from the Federal Bureau of Investigation in New York, New York.

This warrant authorizes the forensic examination of the Target Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

All records on the Target Devices, described in Attachment A, that relate to violations of 18 U.S.C. § 231(a)(3) (obstruction of law enforcement officer related to civil disorder), 18 U.S.C. § 922(g)(5) (possession of a firearm by an illegal alien) and 18 U.S.C. § 2339B (provision of material support to a foreign terrorist organization) (collectively, the "Subject Offenses"), including motive evidence to commit the Subject Offenses, involving DZENAN CAMOVIC his co-conspirators, associates and others with or about whom they have communicated, committed between May 25, 2020 and the present, including:

1. All records and information on the Target Devices including names and telephone numbers, as well as the contents of all call logs, contact lists, text messages, messaging applications (including Facebook, Twitter, and mobile encrypted messaging applications such as WhatsApp), emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, Internet activity (including caches, browser history and cookies, firewall logs, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses), and other electronic media constituting evidence, fruits or instrumentalities of the Subject Offenses.

2. Evidence of user attribution showing who used or owned the Target Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. Evidence regarding the user's state of mind, including whether and why he harbored any hostile views toward law enforcement and the NYPD.

4. Evidence of the user's close associates, including the individuals with whom he may have had contact in the days leading up to June 3, 2020.

5. Evidence indicating efforts to provide support to or promote the activities of terrorists and foreign terrorist organizations, including by committing acts of violence in support of such organizations.

6. Evidence regarding jihadist propaganda, including communications regarding support for extremist attacks and support for violent extremist groups, including al-Qaeda in the Arabian Peninsula and ISIS.

7. Evidence that may identify any additional coconspirators or aiders and abettors, including records that help reveal their whereabouts.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.